particular portion desired and the law enforcement activity for which the record is sought. The Institute also may disclose such a record to a law enforcement agency on its own initiative in situations in which criminal conduct is suspected, provided that such disclosure has been established as a routine use, or in situations in which the misconduct is directly related to the purpose for which the record is maintained;

(8) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification is transmitted to the last known address of such individual;

(9) To either House of Congress, or, to the extent of matter within its jurisdictions, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee;

(10) To the Comptroller General, or any of his or her authorized representatives, in the course of the performance of official duties of the General Accounting Office;

(11) To a consumer reporting agency in accordance with 31 U.S.C. 3711(e); or

(12) Pursuant to an order of a court of competent jurisdiction. In the event that any record is disclosed under such compulsory legal process, the Institute shall make reasonable efforts to notify the subject individual after the process becomes a matter of public record.

(b) Before disseminating any record about any individual to any person other than an Institute employee, the Institute shall make reasonable efforts to ensure that such records are, or at the time they were collected were, accurate, complete, timely, and relevant for Institute purposes. This paragraph (b) does not apply to dissemination made pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552) and paragraph (a)(2) of this section.

§ 1182.14 Procedures for maintaining accounts of disclosures made by the Institute from its systems of records.

(a) The Office of the General Counsel shall maintain a log containing the date, nature, and purpose of each disclosure of a record to any person or to another agency. Such accounting also shall contain the name and address of the person or agency to whom each disclosure was made. This log need not include disclosures made to Institute employees in the course of their official duties, or pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552).

(b) The Institute shall retain the accounting of each disclosure for at least five years after the accounting is made or for the life of the record that was disclosed, whichever is longer.

(c) The Institute shall make the accounting of disclosures of a record pertaining to you available to you at your request. Such a request should be made in accordance with the procedures set forth in § 1182.8. This paragraph (c) does not apply to disclosures made for law enforcement purposes under 5 U.S.C. 552a(b)(7) and § 1182.13(a)(7).

§ 1182.15 Institute responsibility for maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems.

The Chief Information Officer has the responsibility of maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems. These security safeguards shall apply to all systems in which identifiable personal data are processed or maintained, including all reports and outputs from such systems that contain identifiable personal information. Such safeguards must be sufficient to prevent negligent, accidental, or unintentional disclosure, modification or destruction of any personal records or data, and must furthermore minimize, to the extent practicable, the risk that skilled technicians or knowledgeable persons could improperly obtain access to modify or destroy such records or data and shall further insure against such casual entry by unskilled persons without official reasons for access to such records or data.

(a) *Manual systems.* (1) Records contained in a system of records as defined in this part may be used, held, or

stored only where facilities are adequate to prevent unauthorized access by persons within or outside the Institute.

(2) All records, when not under the personal control of the employees authorized to use the records, must be stored in a locked filing cabinet. Some systems of records are not of such confidential nature that their disclosure would constitute a harm to an individual who is the subject of such record. However, records in this category also shall be maintained in locked filing cabinets or maintained in a secured room with a locking door.

(3) Access to and use of a system of records shall be permitted only to persons whose duties require such access within the Institute, for routine uses as defined in §1182.1 as to any given system, or for such other uses as may be provided in this part.

(4) Other than for access within the Institute to persons needing such records in the performance of their official duties or routine uses as defined in §1182.1, or such other uses as provided in this part, access to records within a system of records shall be permitted only to the individual to whom the record pertains or upon his or her written request to the General Counsel.

(5) Access to areas where a system of records is stored will be limited to those persons whose duties require work in such areas. There shall be an accounting of the removal of any records from such storage areas utilizing a log, as directed by the Chief Information Officer. The log shall be maintained at all times.

(6) The Institute shall ensure that all persons whose duties require access to and use of records contained in a system of records are adequately trained to protect the security and privacy of such records.

(7) The disposal and destruction of records within a system of records shall be in accordance with rules promulgated by the General Services Administration.

(b) *Automated systems.* (1) Identifiable personal information may be processed, stored, or maintained by automated data systems only where facilities or conditions are adequate to prevent unauthorized access to such systems in any form. Whenever such data, whether contained in punch cards, magnetic tapes, or discs, are not under the personal control of an authorized person, such information must be stored in a locked or secured room, or in such other facility having greater safeguards than those provided for in this part.

(2) Access to and use of identifiable personal data associated with automated data systems shall be limited to those persons whose duties require such access. Proper control of personal data in any form associated with automated data systems shall be maintained at all times, including maintenance of accountability records showing disposition of input and output documents.

(3) All persons whose duties require access to processing and maintenance of identifiable personal data and automated systems shall be adequately trained in the security and privacy of personal data.

(4) The disposal and disposition of identifiable personal data and automated systems shall be done by shredding, burning, or, in the case of tapes or discs, degaussing, in accordance with regulations of the General Services Administration or other appropriate authority.

§1182.16 Procedures to ensure that Institute employees involved with its systems of records are familiar with the requirements and of the Privacy Act.

(a) The Director shall ensure that all persons involved in the design, development, operation, or maintenance of any Institute system are informed of all requirements necessary to protect the privacy of subject individuals. The Director also shall ensure that all Institute employees having access to records receive adequate training in their protection, and that records have adequate and proper storage with sufficient security to assure the privacy of such records.

(b) All employees shall be informed of the civil remedies provided under 5 U.S.C. 552a(g)(1) and other implications of the Privacy Act, and the fact that the Institute may be subject to civil remedies for failure to comply with the